

SEALED

United States District Court

NORTHERN

DISTRICT OF

U.S. DISTRICT COURT
NORTHERN DISTRICT OF TEXAS

FILED

AUG 25 2015

CLERK, U.S. DISTRICT COURT
By TEXAS
Deputy

In the Matter of the Search of

(Name, address or Brief description of person, property or premises to be searched)

2602/2604 MARTIN LUTHER KING JR.
BLVD. DALLAS, TX 75215, THE LAW
OFFICE OF TSHOMBE A. ANDERSON

**APPLICATION AND AFFIDAVIT
FOR SEARCH WARRANT**

CASE NUMBER: 3:15-MJ- 589 BF

I Special Agent, Kristi Frank, Department of Labor, OIG (DOL-OIG) being duly sworn
depose and say:

I am a(n) Special Agent with the Department of Labor- OIG (DOL-OIG) and have reason to
believe that on the person of or XX on the property or premises known as (name, description and/or location)

(SEE ATTACHMENT A).

in the NORTHERN District of TEXAS there is now concealed a certain
person or property, namely (describe the person or property to be seized)

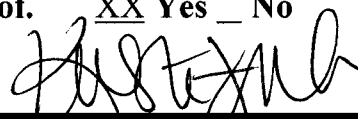
(SEE ATTACHMENT D).

which is (state one or more bases for search and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)

property that constitutes evidence of the commission of a crime, contraband, the fruits of crime, and is,
otherwise, criminally possessed, **concerning a violation of Title 18 United States code, Section(s)**
1341, 1347, 641 and 1957. **The facts to support a finding of Probable Cause are as**
follows:

(SEE ATTACHED AFFIDAVIT OF SPECIAL AGENT KRISTI FRANK).

Continued on the attached sheet and made a part hereof. XX Yes No



Signature of Affiant
KRISTI FRANK
Special Agent, DOL-OIG

Sworn to before me, and subscribed in my presence


August 24, 2015 @ 1:30 P.M.
Date and Time

at

Dallas, Texas
City and State

PAUL D. STICKNEY
United States Magistrate Judge

Name and Title of Judicial Officer



Signature of Judicial Officer

AFFIDAVIT IN SUPPORT OF SEARCH WARRANTS

I, Kristi Frank, a Special Agent with the United States Department of Labor, Office of Inspector General, being duly sworn, state as follows:

AFFIANT'S BACKGROUND

1. I have been employed as a Special Agent with the United States Department of Labor, Office of Inspector General (DOL-OIG), currently assigned to the Dallas Region. I have been a Special Agent for over two years. I have worked with other agents, police officers, and law enforcement personnel who have extensive criminal investigative experience and training. During my tenure as a Special Agent, I have been trained in the execution of search warrants for documents and other evidence in cases involving violations of federal law, including but not limited to: Title 18, United States Code, Section 1347 (Health Care Fraud), Title 18, United States Code, Section 1349 (Conspiracy to Commit Health Care Fraud), and Title 18, United States Code, Sections 1956 & 1957 (Money Laundering). As a Special Agent, my duties included investigating health care fraud, theft of government funds, and money laundering.

2. I am currently assigned to the Dallas, Texas Area Field Office. I am assisting in this investigation by the Department of Labor, Office of Inspector General (DOL-OIG) and the United States Postal Service, Office of Inspector General (USPS-OIG) into Tshombe Anderson, Brenda Anderson, their co-conspirators, and their durable medical equipment companies. As a result of this investigation, Affiant believes the Anderson's and their co-conspirators fraudulently obtained more than \$22,000,000.00.

PROPERTY TO BE SEARCHED

3. This Affiant states that based upon her training, experience, and facts set forth herein, there is probable cause to believe that concealed within
- a. The Law Office of Tshombe A. Anderson, LLC, which is located at 2602 and 2604 Martin Luther King Jr. Blvd, Dallas, TX 75215, more fully described in Attachment A;
 - b. Union Medical Supplies & Equipment LLC located at 2606 Martin Luther King Jr. Blvd, Suite 216, Dallas TX 75215, more fully described in Attachment B;
 - c. The residence of Tshombe and Brenda Anderson, which is located at 2880 S. Serrano Grand Prairie, TX 75054, more fully described in Attachment C;
- are items and information, named and more fully described in Attachment D, that constitute evidence and fruits relating to violations of 18 U.S.C. § 1347 (Health Care Fraud), 18 U.S.C. §641 (Theft of Government Funds), 18 U.S.C. § 1341 (Mail Fraud), 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1956 and 1957 (Money Laundering).¹

PROBABLE CAUSE FOR SEARCH

4. I have probable cause to believe that Tshombe Anderson, Brenda Anderson, Lydia Taylor, Nicole Anderson, Lydia Bankhead, Janet Anderson, Ayyub Anderson, Eric Williams, and Marshea Greer have violated one or more of the following statutes: 18 U.S.C. § 1347 (health care fraud); 18 U.S.C. § 1349 (conspiracy to commit

¹ The initial search and seizure of all these properties will be conducted by agents designated to serve on a filter team in accordance with the guidance, procedures, and protocol provided to them by an AUSA designated to serve on the filter team.

health care fraud); 18 U.S.C. § 1341 (mail fraud); and 18 U.S.C. §§ 1956 and 1957 (money laundering).

5. The statements in this affidavit are based upon my own observations, information provided to me by Special Agents of the USPS-OIG and DOL-OIG, information provided by reliable witnesses, and public source and business records.

6. Because this affidavit is being submitted for the limited purpose of securing search warrants, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to search the properties listed above.

Federal Employees Compensation Act

7. The Federal Employees Compensation Act (FECA) provides monetary compensation, medical care, and vocational rehabilitation to civilian employees of the United States government, including postal workers, who suffer work-related injury or occupational disease in the performance of duty. FECA is administered by the U.S. Department of Labor, Office of Workers' Compensation Programs (OWCP). OWCP offices are located in 12 districts throughout the United States. All monetary and medical benefits to employees are funded by the Employees' Compensation Fund, authorized by 5 U.S.C. § 8147. The Employee's Compensation fund is maintained by appropriations from Congress and is reimbursed for its payouts annually by assessing each federal agency for the amounts paid to its employees in workers' compensation benefits during the previous year.

8. All health care providers providing services through OWCP are required to enroll with Affiliated Computer Services which is OWCP's designated bill processing agent. After enrolling with Affiliated Computer Services, providers may submit claims for payment by OWCP for certain services and durable medical equipment (DME) using an assigned Affiliated Computer Services provider number. By completing and submitting Form OWCP-1168, providers certify that they have satisfied all applicable federal and state licensure and regulatory requirements.

9. In order to receive reimbursement from OWCP, providers must submit Health Insurance Claim Form 1500 (HCFA-1500) seeking payment for services rendered or equipment provided.

10. When an HCFA-1500 is processed and it is determined that payment is warranted, OWCP pays the provider either by check or direct deposit into a bank account designated by the provider. A provider's claims for services to multiple patients and dates of service may be satisfied by a single OWCP payment to the provider.

11. When providers both submit claims to, and accept payment from, OWCP they certify that the service for which reimbursement is sought was performed as described and was necessary, appropriate, and properly billed in accordance with accepted industry standards.

Best First Administration DME of Austin, LLC

12. Union Treatment Center (hereinafter "Union") is a treatment and rehabilitation center with offices in Austin, Corpus Christi, Killeen and San Antonio, Texas. Union specializes in the treatment of injured state and federal worker's

compensation patients. As part of its treatment, Union doctors may prescribe DME (e.g. Biofreeze², crutches, infusion pumps and supplies, and oxygen equipment) for use in the patient's home.

13. Tshombe Anderson worked as an attorney for Union from at least February 2010 to May 2011. In or about February 2010, Tshombe Anderson's wife, Brenda Anderson, began working for Union. Shortly thereafter, Brenda Anderson formed Best First Administration DME of Austin, LLC (BFA) which became Union's in-house DME provider. BFA enrolled officially as a provider with OWCP through Affiliated Computer Services on April 9, 2010. Tshombe Anderson signed the provider enrollment.

14. Once BFA was up and running, a Union doctor would provide Brenda Anderson with a patient's prescription for certain DME items. Brenda Anderson/BFA would then send the prescribed DME to the patient. BFA billed OWCP by submitting an HCFA-1500 through the Affiliated Computer Services account. OWCP would then direct deposit the payment for the DME into BFA's designated bank account.

15. In May 2011, Union fired Brenda and Tshombe Anderson (collectively the "Andersons") as a result of an audit which revealed that they appeared to be engaging in fraudulent billing practices. In June 2011, Union created their own in-house DME company to provide their patients with supplies necessary for treatment. BFA, however, continued to bill OWCP for DME associated with the claims of Union patients.³

² Biofreeze is a brand of medicated ointment/gel that relieves pain when applied to the body.

³ Patients for whom Brenda Anderson obtained OWCP claim information are referred to throughout this affidavit as Union patients, even if they no longer receive treatment at Union.

16. Because BFA is an independent entity enrolled with Affiliated Computer Services and OWCP, Union could not terminate BFA's accounts with Affiliated Computer Services and OWCP when the Andersons were fired.

17. After being fired by Union, the Andersons submitted an amendment to BFA's provider enrollment on July 9, 2011, changing the company's address with OWCP to 2800 E. Whitestone Blvd., Cedar Park, Texas 78713 and designating a new bank account for payment, Bank of America (BOA) account #XXXX1831, which Brenda Anderson opened in May 2011.

The Fraud

18. After the Andersons were terminated, Brenda Anderson retained Union patient records and the OWCP information contained within. BFA continued to bill OWCP for unrequested and/or unnecessary Biofreeze sent to Union patients.

19. From approximately August 2011 through at least February 2015, BFA fraudulently billed for an average of approximately 125 bottles of Biofreeze per month. A review of BFA's mailing procedures, however, indicates that BFA only sent approximately 30 bottles of Biofreeze per month during that same time period.

20. BFA's Cedar Park, Texas address is a private mailbox at a commercial mail receiving agency named PostNet. Brenda Anderson opened an account at PostNet in May 2011. Once a month Brenda Anderson sent PostNet a package that contained approximately 30 smaller packages. PostNet employees would then put postage on the smaller packages, mail them, and charge Brenda Anderson's credit card.

21. Once a month, PostNet forwarded the mail in BFA's private mailbox to an address in Russellville, Arkansas, which surveillance and a witness indicated was Brenda Anderson's home address at the time. In spring 2014, Brenda Anderson called PostNet and requested her forwarding address be changed to 2880 Serrano St. in Grand Prairie, Texas.

22. On November 5, 2014, PostNet in Cedar Park, Texas informed investigators that a package from Brenda Anderson had been received, and, at investigators' request, gave the investigators the opportunity to observe as the package was opened. The outside of the box was addressed to PostNet with a return address of Brenda Anderson at a UPS Store on 990 Hwy 287 N. Mansfield, Texas. Inside the package was another large box with a shipping label from Vitaminerals, a known Biofreeze provider, to Brenda Anderson at 2880 S. Serrano in Grand Prairie, Texas. Inside the large Vitaminerals box were small packages with the return address of BFA at 2800 E. Whitestone Blvd. Cedar Park, Texas; these smaller packages were addressed to 29 different Union patients.

23. PostNet informed investigators that occasionally one of the smaller packages gets returned to PostNet due to an unknown address, and PostNet then forwards it back to Brenda Anderson at 2880 S. Serrano in Grand Prairie, Texas.

Union Medical Supplies & Equipment, LLC (UMSE)

24. On January 14, 2013, Tshombe Anderson used an online Texas Secretary of State Direct Account, obtained by his law firm⁴, to form UMSE. Records indicate that the managers of UMSE are Tshombe Anderson's sister, Lydia Bankhead, and his mother, Marshea Anderson. On March 15, 2013, Lydia Bankhead enrolled the company with Affiliated Computer Services, and listed an office at 327 Cedar Creek Dr., Duncanville, Texas 75137. On April 25, 2013, Tshombe Anderson opened Region's Bank checking account #XXXX5909 for UMSE; he has signature authority on this account.⁵

25. In April 2013, UMSE began fraudulently billing OWCP for DME delivered to the same Union patients as BFA. The first DME packages sent to Union patients by UMSE included a letter that stated DME would be provided by UMSE for their work-related injury at no cost to them. The letter further explained that supplies would cease when billings were denied or when patients sent a written request to UMSE's Cedar Creek Dr. address in Duncanville, Texas.

26. When Union learned that its patients were receiving DME from the Anderson's companies, they informed their patients that they were not supposed to be receiving those supplies, and asked the patients to bring any supplies they received from those providers to Union on their next visit.

27. In January 2014, UMSE changed its address with OWCP to 2606 Martin Luther King Jr. Blvd, Suite 216, Dallas, Texas 75215, an address located next door to

⁴ Tshombe Anderson's law firm, Anderson and Associates, closed in 2012, but the firm's Secretary of State Direct Account remained active after its closure. The Law Office of Tshombe Anderson, LLC opened in September 2013.

⁵ Region's Bank checking account #XXXX5909 was closed January 2014.

The Law Office of Tshombe A. Anderson, LLC, which is located at 2604 Martin Luther King Jr. Blvd, Dallas, Texas 75215. To this day, UMSE packages use 2606 Martin Luther King Jr. Blvd, Suite 216 as the return address. UMSE still claims to operate at this address today.

28. Every DME transaction billed by UMSE since its formation appears to be fraudulent.

Sky-Care Medical Supplies & Equipment, LLC (SMSE)

29. On May 20, 2013, Tshombe Anderson formed Sky-Care Medical Supplies & Equipment, LLC (SMSE) again using his law firm's online Texas Secretary of State Direct Account. Records list Janet Anderson, Tshombe Anderson's sister-in-law, as the manager of SMSE. On July 16, 2013, SMSE was enrolled with the Affiliated Computer Services and listed 4649 Loma Del Sur, Suite 3105, El Paso, Texas 79934 as the address for its office.

30. In August 2013, SMSE began billing OWCP for the same Union patients as BFA and UMSE. Every DME transaction billed by SMSE since its formation appears to be fraudulent.

American Federal Union Claims Advocates, LLC (AFUCA)

31. On January 4, 2014, Tshombe Anderson formed American Federal Union Claims Advocates, LLC (AFUCA) again using Anderson and Associate's online Texas Secretary of State Direct Account. Tshombe Anderson is listed as the only managing member of this company, and the business address is listed at 2604 Martin Luther King Jr. Blvd., Dallas, Texas 75215, which is the same address as The Law Office of Tshombe

A. Anderson, LLC. On March 14, 2014, JPMC account #XXXX8629 was opened in the name of AFUCA with Tshombe Anderson listed as the sole authorized signatory on the account.

Fraudulent Billing by BFA, UMSE, and SMSE

32. Because BFA fails to provide all of the DME for which it bills OWCP, it is engaging in fraudulent billing. OWCP billing records from January 2011 through April 9, 2015 show that 292 patient claim numbers have been billed by at least one of the Andersons' three DME companies. UMSE and BFA have billed OWCP for 84 of the same Union patient claim numbers; UMSE and SMSE have billed 22 of the same Union patient claim numbers; and all three companies have billed 33 of the same Union patient claim numbers.

33. The following are examples of this duplicate billing:

- a. M.P. has sustained many work injuries over time to her hands, knees, feet and shoulders and goes to Union for treatment of her injuries. At some point, she began receiving Biofreeze and electrode pads from BFA that were not requested or needed. Around May 2013, she began also receiving supplies from UMSE. The items, such as a knee brace, could pertain to her injuries; however, they were not the correct size so were completely unusable. She did not need these supplies nor were they requested. She told Union about the unnecessary supplies and that she did not want them. Union told her to refuse the packages, so she did.

The Andersons' DME companies did not bill OWCP for M.P. from May 2011 through February 2012. Then BFA billed throughout 2012 and the beginning of 2013 inflating their bills by approximately three-quarters. UMSE and BFA both billed OWCP for M.P. from April 2013 through July 2013. M.P. did not receive any supplies from July 2013 to February 2014. OWCP, however, was billed for M.P.'s unrequested and unneeded supplies 36 times for a total of \$21,800.00. From August 2013 through April 9, 2015, only UMSE billed OWCP. During that time period, UMSE billed

OWCP 185 times for M.P., for a total fraudulent billing amount of \$124,950.00.

- b. D.Z. injured his back at work in 2006. As of February 2014, he was going to Union for treatment. Union gave him all of the supplies he needed; however, D.Z. also received packages in the mail from UMSE and SMSE containing supplies that were not requested or needed. He told Union about the unnecessary supplies, and they told him to bring the supplies to the office. D.Z. took unopened UMSE and SMSE packages to Union. D.Z. sometimes received duplicate supplies, but he did not receive any supplies in July 2014.

From April 2013 through April 9, 2015, UMSE billed OWCP for D.Z. 165 times for a total of \$106,310.30; SMSE billed OWCP 71 times for a total of \$42,000.00. OWCP has been billed multiple times by UMSE and SMSE for DME devices for D.Z.'s ankle, knee, shoulder, and elbow, although his injury is to his back.

34. From April 11, 2013 through April 9, 2015, UMSE billed approximately \$22,498,085.38 and was paid \$19,573,704.13 by OWCP for DME that was not needed nor requested by the patient or the doctor the patient is seeing. Because UMSE had no authority to provide and bill for DME for Union patients, all funds billed by and paid to UMSE are fraudulent.

35. From August 7, 2013 through April 9, 2015, SMSE billed approximately \$1,833,895.19 and was paid \$1,706,848.19 by OWCP for DME that was not needed nor requested by the patient or the doctor the patient is seeing. Because SMSE had no authority to provide and bill for DME for Union patients, all funds billed by and paid to SMSE are fraudulent.

BFA: Transfer of Fraudulent Proceeds from DOL Deposit Account BOA Acct #XXXX1831 (BFA Master Account)

36. As of June 2011, OWCP began depositing BFA's claim payments into Bank of America (BOA) acct #XXXX1831 (BFA master account). From June 2011 through April 9, 2015, OWCP paid BFA \$733,932.36 on DME claims for Union patients; approximately **\$464,686.00** is fraudulent.

37. Using BOA acct #XXXX1831 (BOA master account), Brenda Anderson purchases DME supplies for BFA and pays for shipping. She also transfers funds into four accounts, which have no other source than BOA acct #XXXX1831 (BFA master account) or each other:

- a. BOA acct #XXXX1873 in the name Best First Administration DME of Austin, LLC Tax Account, from which BFA federal income taxes are paid yearly (BFA tax account);
- b. BOA acct #XXXX7595, held in the names Brenda F. Anderson and Tshombe A. Anderson (BA 1);
- c. BOA acct #XXXX2091, held in the name Brenda F. Anderson (BA 2);
- d. BOA acct #XXXX4261, a savings accounts held in the name Brenda F. Anderson (BA 3).

38. From March 31, 2014 to January 2, 2015, Brenda Anderson transferred \$57,752.00 from BOA acct#XXXX1831 (BFA master account) to BOA acct #XXXX1873 (BFA tax account). Since at least January 2012, BOA acct#XXXX1831 (BFA master account) has been the sole source of funds for BOA acct #XXXX1873 (BFA tax account).

39. From January 2, 2014 to May 12, 2015, Brenda Anderson deposited \$55,000.00 worth of checks written to herself and drawn on BOA acct #XXXX1831 (BFA master account) into BOA acct #XXXX7595 (BA 1); since at least January 2, 2014, the BFA master account and BA 2 are BA 1's only source of funds.

40. From January 2, 2014 to May 12, 2015, Brenda Anderson transferred \$115,500.00 drawn on BOA acct #XXXX1831 (BFA master account) into BOA acct #XXXX2091 (BA 2).

41. From March 25, 2014 to August 17, 2014, Brenda Anderson transferred \$12,000.000 from BOA acct #XXXX1831 (BFA master account) into BOA acct #XXXX4261 (BA 3).

42. Funds often move between BA 1, BA 2, and BA 3. From January 2, 2014 through May 1, 2015, \$53,030.00 moved from BOA acct #XXXX7595 (BA 1) into BOA acct #XXXX2091 (BA 2). Between May 27, 2014 and May 28, 2014, \$8,000 moved from BOA acct #XXXX7595 (BA 1) into BOA acct #XXXX4261 (BA 3). From January 15, 2014 through May 15, 2015, \$3,225 moved from BOA acct #XXXX2091 (BA 2) into BOA acct #XXXX7595 (BA 1). Between July 28, 2014 and September 15, 2014, \$5,525 moved from BOA acct #XXXX2091 (BA 2) into BOA acct #XXXX4261 (BA 3).

UMSE: Transfer of Fraudulent Proceeds from DOL Deposit Account JPMC #XXXX2686 (UMSE Master Account)

43. As of February 20, 2014, OWCP began depositing UMSE's claim payments into JPMC acct #XXXX2686 (UMSE master account) in the name of UMSE.

44. From February 1, 2014 through April 9, 2015, UMSE billed OWCP \$16,764,465.00 and was paid **\$14,499,632.00** into JPMC acct #XXXXX2686 (UMSE master account). All funds in this account originate from UMSE's fraudulent OWCP claim payments. Every seven days, the funds in JPMC acct #XXXXX2686 (UMSE master account) are essentially split between four primary JPMC accounts:⁶

- a. JPMC acct #XXXXX3728 in the name of UMSE (UMSE 1)
- b. JPMC acct #XXXXX8060 in the name of UMSE (UMSE 2)
- c. JPMC acct #XXXXX1318 in the name of UMSE (UMSE 3)
- d. JPMC acct #XXXXX8629 in the name of AFUCA (AFUCA)

Three more accounts occasionally receive funds from JPMC acct #XXXXX2686 (UMSE master account):

- a. JPMC acct #XXXXX8662 in the name Lydia R. Bankhead (LB checking)
- b. JPMC acct #XXXXX6674 in the name Lydia R. Bankhead (LB savings)
- c. JPMC acct #XXXXX7569 in the name Lydia R. Bankhead or Porshea Anderson Taylor (sister P).

45. None of the accounts listed above are funded by an outside source; everything in these accounts originates with OWCP payments to UMSE.

46. From the four accounts listed in a)-d), the funds are dispersed among 13 accounts.

⁶ Three other accounts belonging to Lydia Bankhead receive funds periodically from JPMC account #XXXXX2686 (UMSE master account). They are discussed below because they receive funds from other UMSE-related accounts as well.

47. Between March 13, 2014 and March 26, 2015, a total of **\$285,370.00** was moved in varying increments every seven days from JPMC acct #XXXXX2686 (UMSE master account) to JPMC acct #XXXXX3728 (UMSE 1).

48. Between March 13, 2014 and March 26, 2015, a total of **\$1,197,836.00** was moved in varying increments every seven days from JPMC acct #XXXXX2686 (UMSE master account) to JPMC acct #XXXXX8060 (UMSE 2).

49. Between March 13, 2014 and March 26, 2015, a total of **\$4,127,954.00** was moved in varying increments every seven days from JPMC acct #XXXXX2686 (UMSE master account) to JPMC acct #XXXXX1318 (UMSE 3). Occasionally, funds move from JPMC acct #XXXXX1318 (UMSE 3) to JPMC acct #XXXXX8060 (UMSE 2); a total of \$3,176,244.00 has been moved from JPMC acct #XXXXX1318 (UMSE 3) to JPMC acct #XXXXX8060 (UMSE 2) in the last year.

50. Between March 13, 2014 and March 26, 2015, a total of **\$5,984,014.00** was moved in varying increments every seven days from JPMC acct #XXXXX2686 (UMSE master account) to JPMC acct #XXXXX8629 (AFUCA). The chart below (on the next page) provides an overview of the fund movement described above.

Bank	Bank Account	Name	Opened By	Amount	Money In	Money out
JPMC	(UMSE master account) XXXX2686	UMSE	Bankhead & Tshombe	\$14,499,632.00	From DOL	To JPMC accts 3728, 8060, 1318, 8629, 7569
JPMC	(UMSE 1) XXXX3728	UMSE	Bankhead & Tshombe	\$285,370.00	From JPMC acct 2686	No money out
JPMC	(UMSE 2) XXXX8060	UMSE	Bankhead & Tshombe	\$1,197,836.00	From JPMC acct 2686	To JPMC accts 0278, 6674, 8662, 6457, 7569
JPMC	(UMSE 3) XXXX1318	UMSE	Bankhead & Tshombe	\$4,127,954.00	From JPMC acct 2686	To JPMC acct 8060
JPMC	(AFUCA) XXXX8629	AFUCA	Tshombe Anderson	\$5,984,014.00	From JPMC acct 2686	To JPCM acct 0278

51. Three more accounts occasionally receive funds from JPMC acct #XXXX2686 (UMSE master account): JPMC acct #XXXX8662 in the name Lydia R. Bankhead (LB checking) has received **\$914,709.50** since May 15, 2014; JPMC acct #XXXX6674 in the name Lydia R. Bankhead (LB savings) has received **\$528,454.50** since June 23, 2014; JPMC acct #XXXX7569 in the name Lydia R. Bankhead or Porshea Anderson Taylor, who is Lydia Bankhead's sister, (sister P) received \$87,230.00 total between December 1, 2014 and February 24, 2015.

UMSE: Transfer of Fraudulent Proceeds from JPMC Acct #XXXX8060 (UMSE 2)⁷

52. Lydia Bankhead uses JPMC acct #XXXX8060 (UMSE 2) to disperse money in many different ways, including paying her quarterly federal income taxes and purchasing DME supplies for UMSE, as well as transferring money among bank accounts.

⁷ Please see Exhibit A for an illustration of the money movement out of JPMC acct #XXXX8060.

53. Since June 17, 2014, \$66,912.00 has been transferred from JPMC acct #XXXX8060 (UMSE 2) to JPMC checking acct #XXXX6457⁸ in the name Lydia R. Taylor, who is Lydia Bankhead's niece.

54. Between April 4, 2014 and August 11, 2014, JPMC acct #XXXX8060 (UMSE 2) transferred \$228,006.00 to Lydia Bankhead's JPMC checking acct #XXXX8662 (LB checking).

55. Between May 8, 2014 and September 30, 2014, JPMC acct #XXXX8060 (UMSE 2) transferred \$63,224.00 to Lydia Bankhead's JPMC savings acct #XXXX6674 (LB savings).

56. Between October 3, 2014 and February 2015, JPMC savings acct #XXXX6674 (LB savings) transferred \$374,500 in seven periodic transactions to JPMC checking acct #XXXX8662 (LB checking). The checking account is used to pay for daily expenses to stores such as Kroger, Walmart, and Amazon.com to pay off Lydia Bankhead's credit card, and to pay off a black Lexus RX450, VIN #JTJZB1BA7E2009557; however it occasionally transfers money back to the savings account and to other bank accounts.

57. Between September 30, 2014 and February 9, 2015, JPMC checking acct #XXXX8662 (LB checking) transferred \$178,000 into Lydia Bankhead's savings account (JPMC savings acct #XXXX6674) (LB savings).

⁸ Lydia Taylor also receives money into her JPMC checking acct #XXXX6457 from SMSE. The disposition of these funds is discussed in the SMSE section below.

58. From April 3, 2014 through March 14, 2015, Lydia Bankhead wrote herself \$186,000.00 worth of checks on JPMC checking acct #XXXX8662 (LB checking) and deposited those into her Arvest Bank checking acct #XXXX6805.

59. Between May 8, 2014 and January 28, 2015, Lydia Bankhead also wrote herself \$37,500.00 worth of checks on JPMC checking acct #XXXX8662 (LB checking) and deposited those into her Arvest Bank savings acct #XXXX6915.

60. On August 18, 2014, JPMC acct #XXXX8060 (UMSE 2) transferred \$10,000 to Lydia Bankhead and Porshea Taylor's JPMC acct #XXXX7569 (sister P). Between October 27, 2014 and January 28, 2015, Lydia Bankhead's JPMC savings account #XXXX6674 (LB savings) transferred \$30,000.00 to Lydia Bankhead and Porshea Taylor's JPMC acct #XXXX7569 (sister P).

UMSE: Transfer of Fraudulent Proceeds from JPMC Acct #XXXX8629 (AFUCA)

61. From JPMC acct #XXXX8629 (AFUCA), funds move into three accounts, two of which belong to Anderson's law practice:

- a. JPMC acct #XXXX0278 in the name of The Law Office of Tshombe A. Anderson, LLC (law office 1);
- b. JPMC acct #XXXX9265 in the name of The Law Office of Tshombe A. Anderson, LLC (law office 2); and
- c. JPMC acct #XXXX0660 in the name of Tshombe Anderson (TA personal account).

62. Between September 4, 2014 and February 24, 2015, **\$1,574,421.00** was wired from JPMC acct #XXXX8629 (AFUCA) to JPMC acct #XXXX0278 (law office 1).

63. Between September 4, 2014 and February 12, 2015, **\$260,000.00** was wired from JPMC acct #XXXX8629 (AFUCA) to JPMC acct #XXXX9265 (law office 2).

64. Between July 24, 2014 and February 12, 2015, **\$105,000.00** was wired from JPMC acct #XXXX8629 (AFUCA) to JPMC acct #XXXX0660 (TA personal account).

65. On or about March 2014, Tshombe Anderson signed two checks, dated March 19, 2014, to his law office totaling \$1,071.03 drawn on JPMC acct #XXXX8060 (UMSE 2) and deposited into JPMC acct #XXXX0278 (law office 1); Tshombe Anderson signed three checks, dated March 21, 2014, to his law office totaling \$4,100.00 drawn on JPMC acct #XXXX8060 (UMSE 2) and deposited into JPMC acct #XXXX0278 (law office 1).

SMSE: Transfer of Fraudulent Proceeds from DOL Deposit Account BOA Acct #XXXX6213

66. As of August 15, 2013, OWCP began depositing SMSE's claim payments into Bank of America (BOA) acct #XXXX6213 (SMSE master account) in the name of UMSE.

67. From August 15, 2013 through April 9, 2015, SMSE billed OWCP \$1,833,895.19 and was paid **\$1,706,848.19** into BOA acct #XXXX6213 (SMSE master account). All funds in this account originate from SMSE's OWCP claim payments. The funds in BOA acct #XXXX6213 (SMSE master account) are then transferred to two SMSE accounts: BOA acct #XXXX2317 (SMSE 1) and BOA acct #XXXX0710 (SMSE

2); all funds in SMSE 1 and 2 originate from the SMSE master account and are therefore fraudulent proceeds.

68. Between January 2, 2014 and May 11, 2015, **\$555,158.00** was transferred from BOA acct #XXXX6213 (SMSE master account) to BOA acct #XXXX2317 (SMSE 1). Occasionally, funds in BOA acct #XXXX2317 (SMSE 1) move into BOA acct #XXXX0710 (SMSE 2); from April 10, 2014 to April 1, 2015, \$416,365.00 moved from SMSE 1 to SMSE 2.

69. Between January 2, 2014 and May 11, 2015, **\$917,271.00** was transferred from BOA acct #XXXX6213 (SMSE master account) to BOA acct #XXXX0710 (SMSE 2). From BOA acct #XXXX0710 (SMSE 2), funds are transferred to Janet Anderson, who is Lydia Bankhead's sister-in-law; to Lydia Taylor; to Tshombe Anderson's law firm through JPMC acct #XXXX0278 (law office 1); and to Lydia Bankhead's Arvest Bank checking acct #XXXX6805.

70. Between October 3, 2014 and May 8, 2015, **\$188,000.00** has moved from BOA acct #XXXX0710 (SMSE 2) to Janet Anderson's BOA acct #XXXX1695; since September 2014, funds in BOA acct #XXXX1695 have been the sole source of funding for Janet and Ayyub Anderson's BOA acct #XXXX1167, which received \$87,000 between September 26, 2014 and July 11, 2015. From BOA acct #XXXX1167, Janet Anderson writes checks to herself and to her husband which are then deposited into a Navy Federal Credit Union account, where the fraud proceeds are comingled with Ayyub Anderson's legitimate government contractor salary.

71. From BOA acct #XXXX0710 (SMSE 2), funds are also transferred to Lydia Taylor's JPMC checking acct #XXXX6457. From July 25, 2014 through March 19, 2015, **\$195,824.00** has been moved from SMSE 2 to Lydia Taylor's JPMC checking account. From June 13, 2014 through April 10, 2015, the total deposited into Lydia Taylor's JPMC checking acct #XXXX6457 from UMSE 2 and SMSE 2 is **\$262,736.00**. From June 18, 2014 through April 10, 2015, Lydia moved \$101,460.51 from her JPMC checking acct #XXXX6457 to her JPMC savings acct #XXXX0588. From her JPMC savings acct #XXXX0588, Lydia Taylor obtained a \$41,500 cashier's check, which she used to purchase a 2014 Jeep Grand Cherokee VIN 1C4RJEBG9EC521848 at a Frisco, Texas dealership. An analysis of Lydia Taylor's bank records and the Texas Workforce Commission indicate that she does not have any legitimate source of income.

72. Between December 19, 2013 and May 15, 2014, BOA acct #XXXX0710 (SMSE 2) transferred \$72,426 to JPMC acct #XXXX0278 in the name of The Law Office of Tshombe A. Anderson, LLC (law office 1).

73. Between January 13, 2014 and May 15, 2014, BOA acct #XXXX0710 (SMSE 2) transferred \$57,965 to Lydia Bankhead's Arvest Bank checking acct #XXXX6805.

74. The chart below (on the next page) summarizes the movement of SMSE fraudulent proceeds as described above:

Bank	Bank Account	Name on Account	Opened By	Amounts	\$ In from	\$ out to
Bank of America	(SMSE master account) XXXX6213	SMSE	Janet Anderson	\$1,706,848.19	From DOL	BOA accts 0710, 2317
Bank of America	(SMSE 1) XXXX2317	SMSE	Janet Anderson	\$555,158.00	From BOA acct 6213	BOA acct 0710
Bank of America	(SMSE 2) XXXX0710	SMSE	Janet Anderson	\$917,271.00	From BOA acct 6213, 2317	BOA accts 6213, 1695, 2317; JPMC accts 6457, 0588, 0278; Arvest acct 6805
Bank of America	XXXX1695	Janet Anderson	Janet Anderson	\$188,000.00	From BOA acct 0710	BOA acct 1167
Bank of America	XXXX1167	Janet and Ayyub Anderson	Janet and Ayyub Anderson	\$87,000.00	From BOA acct 1695	Transfers to NFCU

The Law Office of Tshombe A. Anderson, LLC located at 2604 Martin Luther King Jr. Blvd., Dallas, Texas & the UMSE Office located at 2606 Martin Luther King Jr. Blvd, Suite 216, Dallas Texas 75215

75. On September 27, 2013, Tshombe Anderson formed The Law Office of Tshombe A. Anderson, LLC. Previously, Tshombe Anderson's law office was called Anderson & Associate's. The name change appears to coincide with disciplinary action that was taken by the State Bar of Texas against Tshombe Anderson. Tshombe Anderson is listed as the only managing member of this law office, and the business address is listed at 2604 Martin Luther King Jr. Blvd., Dallas, Texas 75215. J.P. Morgan Chase (JPMC) accounts #XXXX0278 and #XXXX9265 were opened in the name of The Law Office of Tshombe A. Anderson, LLC, and Tshombe Anderson is the sole authorized signatory on these accounts.

76. Surveillance indicates that Tshombe Anderson goes to the law office location regularly. A trash run conducted on April 17, 2014 examined all the trash in the

dumpster used by the entire strip mall where the law office is located. A lot of shred bags were present, but their origin and contents are unknown.

77. The trash run uncovered the first page of a four page March 2014 bank statement for JPMC acct #XXXX8629 in the name AFUCA (AFUCA). The AFUCA account was opened March 14, 2014 using \$10,000.00 of unknown origin, and this was the first page of the first account statement. The statement showed a beginning balance of \$0.00 and an ending monthly balance of \$395,321.00. The statement further showed four separate online transfers on March 20, 2014 from JPMC acct #XXXX2686 (UMSE master account) to the AFUCA account, in the amounts of \$107,820.00; \$105,475.00; \$102,685.00; and \$84,034.00. The statement showed that same day, an online transfer of \$84,034.00 was made from the AFUCA account to the JPMC acct #XXXX0278 in the name of The Law Office of Tshombe A. Anderson, LLC (law office 1). The statement further showed another online transfer from the UMSE master account to the AFUCA account occurred on March 27, 2014 in the amount of \$69,341.00.

78. In addition to the partial bank statement, an empty Priority Mail envelope from Janet Anderson addressed to the Law Firm of Anderson & Associates (the former name of Tshombe Anderson's law firm) was located in the trash.

79. Additional surveillance shows that 2602 Martin Luther King Jr. Blvd, the address for AFUCA on bank statements, and 2604 Martin Luther King Jr. Blvd, the address for The Law Office of Tshombe A. Anderson, are not separate spaces but have been combined into a single or shared office space. From the front of the building, both

2602 and 2604 have signs on their doors indicating they are part of The Law Office of Tshombe A. Anderson.

80. Currently, J.P. Morgan Chase Bank has 2602 Martin Luther King Jr. Blvd, Dallas, Texas 75215 as the address of record for JPMC acct #XXXX8629 (AFUCA); the Texas Secretary of State has AFUCA's address listed as 2604 Martin Luther King Jr. Blvd. Both 2602 and 2604 are addresses for The Law Office of Tshombe A. Anderson.

81. UMSE's address is 2606 Martin Luther King Jr. Blvd., Suite #216, which is an upstairs suite in the same building as 2602 and 2604. In January 2015, investigators visited suite 216 in the early afternoon. The entrance to Suite 216 is located in an interior hallway upstairs from Tshombe Anderson's law office. Suite 216 has a solid brown/wooden door bearing a plaque with the name "Union Medical Supplies & Equipment, LLC." clearly written over two lines. An investigator knocked on the door, but there was no answer. An uninterested witness who works in the office across the hall from Suite 216, looked out her office's door when she heard the knock across the hall; she described Suite 216 to the investigator as an empty suite owned by the law office downstairs.

82. As described above, the return address on UMSE packages was 2606 Martin Luther King Jr Blvd., Suite #216. On August 7, 2015, investigators interviewed a postal carrier who was assigned for more than a year to the mail route that delivers to the UMSE empty office and The Law Office of Tshombe Anderson located at 2602/2604 Martin Luther King Jr. Blvd. In response to investigators' questions about UMSE packages being marked "return to sender", she stated: "It's a fraud! The parcels being

returned belong to the attorney downstairs, Mr. Tshombe Anderson, it's his medical company." She also explained that initially she attempted to deliver UMSE parcels marked "refused" or "return to sender" to the suite above Tshombe Anderson's law office, but the office was always vacant and no one ever answered the door to take delivery. As a result, those parcels were sent to dead mail per postal regulations. Later on, she was informed that Tshombe Anderson would accept delivery of those packages downstairs at his law office. In her current position as a mail sorter, the postal worker stated that within the last week she has personally seen two return to sender parcels marked "refused" or "return to sender" for the UMSE address above Tshombe Anderson's law office.

83. Bank records for JPMC accounts #XXXX0278, #XXXX1788, and #XXXX9265 opened and held in the name of The Law Office of Tshombe A. Anderson, LLC, for which Tshombe Anderson is the sole authorized signatory, were reviewed as a part of this investigation.⁹ A review of these records showed that the vast majority of expenditures from these accounts were for personal expenses, and very few business related expenditures.

Other Properties Involved

2880 S. Serrano Grand Prairie, Texas 75054

84. As described above, from June 2011 through January 2015, Brenda Anderson billed approximately 30 of the same claimants every Tuesday for one unit of

⁹ In accordance with proper procedures, the bank records were provided to Affiant after a filter team had thoroughly vetted the records and removed any potentially privileged information.

Biofreeze charging \$125.00 per item. In this same time period, Brenda Anderson billed OWCP for 4,255 bottles of Biofreeze for a total of \$572,286.00. The Biofreeze was at least partially obtained from Vitaminerals.

85. Approximately 52 invoices from Vitaminerals were reviewed. Vitaminerals charges approximately \$7.60 per bottle of Biofreeze. From June 2011 through November 18, 2014, Brenda Anderson purchased 1,186 bottles of Biofreeze, paying a total of \$9,289.25. The last 5 invoiced orders (6/24/2014, 7/25/2014, 9/1/2014, 10/7/2014, 11/18/2014) were shipped to 2880 S. Serrano Grand Prairie, Texas 75054, which is her current residential address.

86. Beginning February 1, 2015, OWCP stopped accepting the code Brenda Anderson had been using to bill the Biofreeze at \$125. Immediately after this change, Brenda Anderson attempted to bill OWCP 10 times in the month of February 2015 for Biofreeze at \$125 per bottle. All bills were denied.

87. In March 2015, Brenda Anderson changed her strategy and began fraudulently billing OWCP using a high-value DME code for a type of garment BFA began sending Union patients; none of these patients had a prescription for such a garment nor a use for one. Brenda Anderson fraudulently billed OWCP \$2,500.00 dollars per garment, for a total of \$25,000.00 in March 2015 alone.

88. On May 11, 2015, D.T., a Union patient, was interviewed regarding her receipt of one of these garments from BFA. D.T. was injured on the job in June 2007 and went to Union for treatment. D.T. receives treatment at Union every three months and receives all necessary medical supplies from them. D.T. still receives Biofreeze

approximately once a month from BFA, which she did not request or need. D.T. has received DME from UMSE and SMSE in the past, which she did not request or need. D.T. takes unopened packages from BFA, UMSE and SMSE to Union.

89. D.T. provided the last package she received in the mail from BFA, on or about May 8, 2015. The package was addressed to D.T. with a return address for BFA at the PostNet location. The package contained one bottle of Biofreeze and one compression glove. On May 8, 2015, BFA billed OWCP \$2,500.00 for one garment (the unneeded compression glove) provided to D.T.

90. The compression glove supplier is a company named Tenspros. Invoices from this company show that Brenda Anderson is ordering these supplies online through BFA. Brenda Anderson placed orders from this company on February 17, 2015, April 27, 2015, and May 30, 2015. Tenspros ships the ordered supplies to Brenda Anderson's residence at 2880 S. Serrano, Grand Prairie, Texas.

91. Currently, the 2880 S. Serrano, Grand Prairie, Texas is the address on record at Bank of America for the BOA acct #XXXXX1831 (BFA master account); BOA acct #XXXXX1873 in the name Best First Administration DME of Austin, LLC Tax Account, from which BFA federal income taxes are paid yearly (BFA tax account); BOA acct #XXXXX7595, held in the names Brenda F. Anderson and Tshombe A. Anderson (BA 1); BOA acct #XXXXX2091, held in the name Brenda F. Anderson (BA 2); and BOA acct #XXXXX4261, a savings accounts held in the name Brenda F. Anderson (BA 3).

1422 Lands End Point North, Russellville, AR 72802

92. The investigation determined that Stamps.com was the primary postage provider used by the Andersons to mail packages of DME to Union patients. Throughout the investigation, the account and tracking numbers provided by Stamps.com have been monitored. The USPS track and confirm database was queried by inputting the tracking number on the package label or from Stamps.com to ascertain the first scan point location for each package mailed by UMSE to OWCP claimants.

93. The initial scan for packages sent by UMSE was completed at the Little Rock Processing & Distribution Center, Little Rock, Arkansas 72206. Lydia Bankhead and her mother, Marshea Anderson, resided at 2104 Skyline Dr., Russellville, Arkansas 72802 until approximately January 2014. In January 2013, a change of address request was filed to forward UMSE mail from 327 Cedar Creek, Duncanville, Texas to 2104 Skyline, Russellville, Arkansas 72802.

94. Initially the scan for packages sent by SMSE was done at a post office in White Sands Missile Range, NM. At that time, investigative activity revealed that Janet Anderson and her husband Ayyub Anderson resided at 416 Zeus, White Sands Missile Range, New Mexico.

95. In December 2013, the Russellville, Arkansas post office confirmed that about once a week for the last few months, a black female driving a silver SUV dropped off a wire container full of mail. the postal clerk remembered being suspicious of the mailings because the return address was listed in Texas.

96. In December 2013, a USPS rural carrier in Russellville, Arkansas confirmed that Lydia Bankhead and Marshea Anderson resided at 2104 Skyline Dr. and that Lydia Bankhead often received mail with the word "medical" written in the return address and that Lydia Bankhead and Tshombe Anderson received mail for Union Medical Supplies & Equipment on numerous occasions.

97. In January 2014, Lydia Bankhead notified OWCP that UMSE was changing its address to 2606 Martin Luther King Jr. Blvd Suite 216 Dallas, Texas. This unit is located above Tshombe Anderson's law firm. Surveillance in January 2014 showed no activity at this unit.

98. In March 2014, Lydia Bankhead and Marshea Anderson moved to 1422 Lands End North, Russellville, Arkansas 72802.

99. Stamps.com provided an IP address of 173.216.123.143 used to access the SMSE account on October 30, 2014. The same IP address was used to access the UMSE account on November 5, 2014. A subpoena to Suddenlink confirmed that the IP address 173.216.123.143 was registered to Lydia Bankhead at 1422 Lands End Point North, Russellville, Arkansas 72802.

100. Surveillance from March 16, 2015 through March 18, 2015 did not show any residents at 2104 Skyline Dr. However, it did show Lydia Bankhead leaving her residence at 1422 Lands End Point North in a Dark Lexus SUV license plate 742 TWH to go to the residence at Skyline Dr. where she briefly checked the mail and then left.

101. On March 27, 2015, a woman matching Lydia Bankhead's description and driving a Lexus SUV with license plate 742 TWH dropped off packages at the

Russellville Post Office with return addresses to UMSE in Dallas, Texas. Packages with an SMSE return address were also being dropped at the Russellville Post Office.

102. “The Brace Shop,” a large supplier for UMSE, provided an IP address of 173.216.47.29 for UMSE orders placed on June 16, June 18, and June 20, 2015. A subpoena to Suddenlink confirmed that the IP address 173.216.47.29 accessed on the dates and times of these orders is registered to Lydia Bankhead, 1422 Lands End Point North, Russellville, Arkansas 72802.

Seizure of Computer and Electronic Data

103. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static--that is, long-term—IP addresses, while other computers have dynamic—that is frequently changed—IP addresses.
- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, floppy disks, flash memory, CD-ROMs, and several other types of magnetic or optical media not listed here.

104. In the present case, your affiant requests permission to search and seize records, including that which may be stored on a computer. Your affiant also requests permission to seize the computer hardware that may contain such records if it becomes necessary for reasons of practicality to remove the hardware and conduct a search off-site. Based on first-hand knowledge as well as information provided by my investigative partners, computers are being used by BFA, UMSE and SMSE in relation to the crimes being investigated, and based on the almost universal presence and use of computers in American businesses, including medical businesses, at this time, your affiant believes that, in the present case, computer hardware is a container for evidence, was itself an instrumentality of the crime under investigation, and may be a container for contraband.

105. Based upon my training and experience as a Special Agent, as well as information related by other law enforcement officers, I am aware that persons who commit mail and wire fraud often maintain records and proceeds of their fraudulent activity, as well as financial documents, such as bank statements, cancelled checks and savings account information, at their personal residences and in their vehicles.

106. Based on my knowledge, training, and experience, I know that computer hardware, software, documentation, passwords, and data security devices may be important to a criminal investigation in two distinct respects: (1) the items themselves may be instrumentalities, fruits, and/or evidence of crime; and/or (2) items may have been used to collect and store information about crimes (in the form of electronic data).

107. As described above, this application seeks permission to search and seize records that might be found at the Law Office of Tshombe A. Anderson, LLC, which is

located at 2602 and 2604 Martin Luther King Jr. Blvd, Dallas, TX 75215, Union Medical Supplies & Equipment LLC located at 2606 Martin Luther King Jr. Blvd, Suite 216, Dallas TX 75215, and the residence of Tshombe and Brenda Anderson, which is located at 2880 S. Serrano Grand Prairie, TX 75054, in whatever form they are found. I submit that if a computer or electronic medium is found on the premises, there is probable cause to believe those records will be stored in that computer or electronic medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the internet. Electronic files downloaded onto a hard drive can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using readily available forensics tools. This is so because when a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, the data remains on the hard drive until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space-that is, in space on the hard drive that is not currently being used by an active file-for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.
- c. Wholly apart from user-generated files, computer storage media-in particular, computers' internal hard drives-contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the internet are sometimes automatically downloaded into a temporary internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to

those files, and the files are only overwritten as they are replaced with more recently viewed internet pages or if a user takes steps to delete them.

108. This application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer located at the Law Office of Tshombe A. Anderson, LLC, which is located at 2602 and 2604 Martin Luther King Jr. Blvd, Dallas, TX 75215, Union Medical Supplies & Equipment LLC located at 2606 Martin Luther King Jr. Blvd, Suite 216, Dallas TX 75215, and the residence of Tshombe and Brenda Anderson, which is located at 2880 S. Serrano Grand Prairie, TX 75054, because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
- b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing,

such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

- c. A person with the appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

109. In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media.

Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

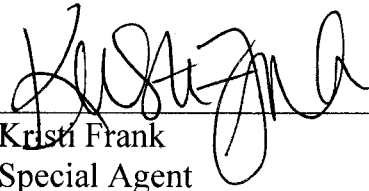
- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

110. Based on the foregoing, and consistent with Rule of Criminal Procedure 41(e)(2)(B), when persons executing the warrant conclude that it would be impractical to review the media on-site, the warrant I am applying for would permit seizing or imaging storage media that reasonably appear to contain some or all of the evidence described in the warrant, thus permitting its later examination consistent with the warrant. The examination may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

111. In light of these concerns, I hereby request the Court's permission to seize the computer hardware (and associated peripherals) that are believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the hardware for the evidence, described, if, upon arriving at the scene, the agents executing the search conclude that it would be impractical to search the computer hardware on-site for this evidence.


CONCLUSION

112. Based on the preceding information, there is probable cause to believe that the named items and information more fully described in Attachment D, constituting evidence or fruits of violations of 18 U.S.C. § 1347 (Health Care Fraud), 18 U.S.C. § 641 (Theft of Government Funds), 18 U.S.C. § 1341 (Mail Fraud), 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1956 and/or 1957 (Money Laundering), will be found in the suspected premises more fully described in Attachments A – C.



Kristi Frank
Special Agent
United States Department of Labor
Office of Inspector General

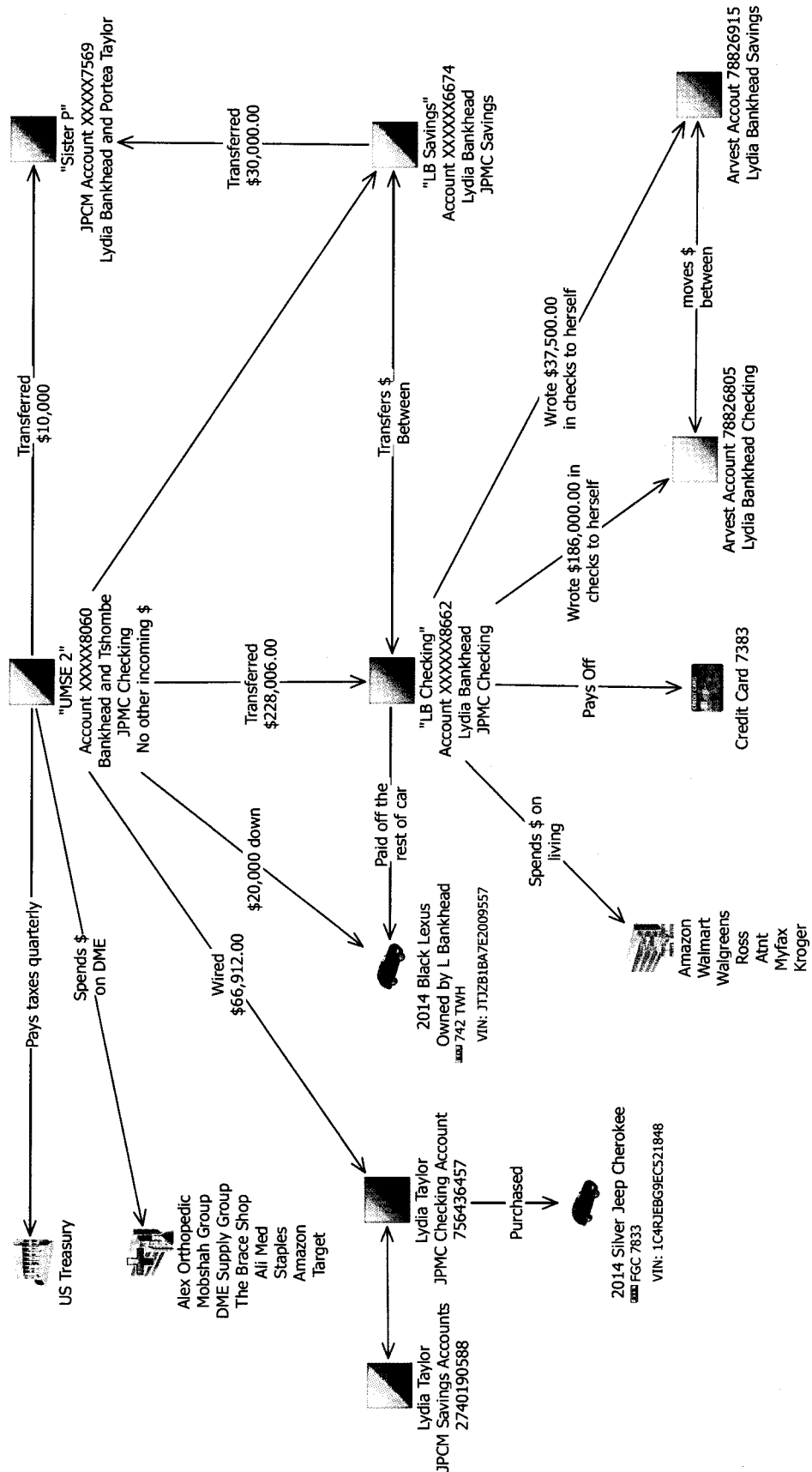
Subscribed and sworn to before me on August 25, 2015, and I find probable cause.



Paul D. Stickney
United States Magistrate Judge

EXHIBIT A

Movement of Funds from January 2014 through March 14, 2015 out of JPMC 8060



ATTACHMENT A

DESCRIPTION OF SUSPECTED PLACE AND PREMISES TO BE SEARCHED

The Law Office of Tshombe A. Anderson, LLC, is located at 2602 and 2604 Martin Luther King Jr. Blvd, Dallas, TX 75215. The law office is located on the corner of Martin Luther King Jr. Blvd and Atlanta St. The law office is the end office on a strip mall. The front has a large sign displaying the name of the office and telephone number. Both doors (2604 and 2602) have signs on them for the law office. The front of the building is grey cement.



ATTACHMENT B

DESCRIPTION OF SUSPECTED PLACE AND PREMISES TO BE SEARCHED

The office leased to UMSE is located at 2606 Martin Luther King Jr. Blvd. Suite 216, Dallas, TX 75219. The entry to 2606 is a glass door on the first floor. Once you enter, there is an elevator. Take the elevator up one floor to floor 2. There, is a large wooden door with a sign stating "Union Medical Supplies & Equipment, LLC" which can be seen when exiting the elevator.



ATTACHMENT C
DESCRIPTION OF SUSPECTED PLACE AND PREMISES TO BE SEARCHED

The residence of Tshombe and Brenda Anderson is a single family residence located at 2880 S. Serrano St., Grand Prairie, TX 75054. It is a light tan stone and brick exterior. The residence has a two car garage with a small roof over the garage door closest to the front door. There is a second story front patio. The front door entryway is covered and has a brown door with a window above it. There is a light brown privacy fence surrounding the backyard.



**ATTACHMENT D
ITEMS TO BE SEIZED**

Any and all of the following named items and information relating to BFA, UMSE or SMSE and its associated clinics, including, relating to violations of 18 U.S.C. § 1347 (Health Care Fraud), 18 U.S.C. § 641 (Theft of Government Funds), 18 U.S.C. § 1341 (Mail Fraud), 18 U.S.C. § 1343 (Wire Fraud), and 18 U.S.C. § 1957 (Money Laundering) for the period June 1, 2010, through the date of the execution of the search warrant in this matter. This information may be stored or filed, and includes any format in which the information may exist.

1. All documents constituting, concerning, or relating to: patient files and treatment, including but not limited to: physician evaluations and assessments, including drafts and edited versions; therapy notes; daily treatment notes; treatment, billing, and coding worksheets and spreadsheets; physician, chiropractor, and therapist orders and instructions; communication notices, notes, and memorandum to staff, employees, patients, physicians, chiropractors, therapists, UMSE or SMSE owners, case managers, billing agents or representatives, and patients; therapy or treatment notes and instructions; patient admission and discharge; referrals from physicians, patient and employee payment or expense logs; patient progress notes; DOL-OWCP pre-authorization records and communications; certificates of medical necessity; prescriptions; dispensing orders; orders for durable medical equipment; explanations of medical benefits; patient complaints or other communications including those related to treatment, services, benefits, money, cash, employees, and patient instructions or education about participation in the DOL-OWCP program.
2. All items appearing to be durable medical equipment.
3. All boxes and packaging appearing to be used for the shipment of durable medical equipment.
4. All documents constituting, concerning, or relating to: the submission of claims for reimbursement to DOL-OWCP and other medical insurance providers, and receipt of payments from such, including but not limited to: hard copy faxes, and email faxes, super-bills, communication including emails, notices, memorandum and instructions related to the submission of claims, OWCP Forms OWCP-1168,

OWCP-1500, HCFA-1500, and related forms, supporting documentation, including drafts and edited versions.

5. All documents constituting, concerning, or relating to: the DOL-OWCP program, including and not limited to: manuals, newsletters, bulletins, publications, advisories, policies and procedures, correspondence, cancelled checks, and notices of over-payment.
6. All past and current employee and contractor personnel files, including but not limited to: licenses, certifications, training and education, employee handbooks or manuals, organizational charts, payroll records, cancelled checks, bonus payments or logs, employment and compensation agreements and records, W-2s, 1099s, work schedules, disciplinary records, unemployment commission records, termination notices and warnings, and job descriptions.
7. All contracts, agreements, or other documents including financial records, related to the provision of health care services by providers other than BFA, UMSE or SMSE and its offices, including but not limited to compensation agreements, kick-backs, solicitations, receipt of remunerations, cancelled checks, payment logs, and bank account information.
8. All brochures and advertising materials related to the promotion of BFA, UMSE or SMSE and its offices, including but not limited to: items related to the BFA, UMSE or SMSE fairs, websites, business cards, pamphlets, and other literature.
9. Financial books, records, and documents constituting, concerning, or relating to payments from UMSE OR SMSE and its offices to employees, referral sources, physicians, chiropractors, and outside providers of health care services.
10. Any information described in the proceeding paragraphs stored in electronic or magnetic media, electronic data processing and storage devices, computers and computer systems, including central processing units, internal and peripheral storage devices such as fixed disks, external hard disks, thumb drives, flash drives, floppy disk drives and diskettes, tape drives and tapes, optical storage devices such as modems, together with system documentation, operating logs and documentation, software and instruction manuals. Any and all records showing or bearing indicia of the use, ownership, possession or control of the computer

equipment, accessories, telephone(s) and modems(s) such as usernames, passwords, invoices or warranty registrations. Any and all tapes, cassettes, hardware, computer disks, data disks, magnetic media, thumb drives, flash drives, floppy disk, tape systems, CD ROM disks, optical data storage media, hard disks and other computer relationship operational equipment.

- a) Your affiant knows that computer hardware, software, and electronic files may be important to a criminal health care fraud investigation in two distinct ways: (1) the objects themselves may be contraband, evidence, instrumentalities, or fruits of crime, and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data. Rule 41 of the Federal Rules of Criminal Procedure permits the government to search for and seize computer hardware, software, and electronic files that are evidence of crime, contraband, instrumentalities of crime, and/or fruits of the crime.
- b) In the present case, your affiant requests permission to search and seize records, including that which may be stored on a computer. Your affiant also requests permission to seize the computer hardware that may contain such records if it becomes necessary for reasons of practicality to remove the hardware and conduct a search off-site. Based on first-hand knowledge as well as information provided by my investigative partners, computers are being used by BFA, UMSE and SMSE in relation to the crimes being investigated, and based on the almost universal presence and use of computers in American businesses, including medical businesses, at this time, your affiant believes that, in the present case, computer hardware is a container for evidence, was itself an instrumentality of the crime under investigation, and may be a container for contraband.
- c) Based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices including hard disk drives, floppy disks, compact disks, magnetic tapes and memory chips. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

- i. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched.
- ii. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.
- iii. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 160 gigabytes (GB) of data are now commonplace in desktop computers. Consequently, each non-networked, desktop computer found during a search can easily contain the equivalent of 80 million pages of data, which, if printed out, would result in a stack of paper over four miles high. Further, a 160 GB drive could contain as many as approximately 150 full run movies or 150,000 songs.

iv. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband or instrumentalities of a crime.

d) The computer forensic examiner will attempt to create an electronic "image" of all computers that are likely to store the evidence described in the warrant. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Imaging a computer permits the agents to obtain a forensic copy of the computer's stored data without actually seizing the computer hardware. The computer forensic examiner or another technical expert will then conduct an off-site search for the evidence described in the warrant from the image copy at a later date.

11. If "imaging" proves impractical, or even impossible for technical reasons, then Affiant hereby requests the Court's permission to seize those components of the computer system that the computer forensic examiner believes must be seized to permit the agents to locate the evidence described in the warrant. The components will be seized and taken into the custody of the agent. The computer forensic examiner or another technical expert will then conduct an off-site search for the evidence described in the warrant at a later date. If employees of BFA, UMSE or SMSE so request, the computer forensic examiner will, to the extent practicable, attempt to provide the employees with copies of any files not within the scope of

the warrant that may be necessary or important to the continuing function of BFA, UMSE or SMSE's legitimate business. If, after inspecting the computers, the analyst determines that some or all of this equipment is no longer necessary to retrieve and preserve the evidence, the government will return it within a reasonable time.

12. Searching the computer system for the evidence described above will require a range of computer forensic analysis techniques. Criminals can mislabel or hide files and directories; encode communications to avoid using key words; attempt to delete files to evade detection; or take other steps designed to frustrate law enforcement searches for information. In order to properly execute the search authorized by the warrant, specially trained agents or forensic analysts will be required to conduct a thorough forensic analysis of the seized media, such as scanning areas of the disk not allocated to listed files, or opening every file and scanning its contents briefly to determine whether it falls within the scope of the warrant. In light of these difficulties, your affiant requests permission to use whatever computer forensic analysis techniques appear necessary to locate and retrieve the above-described evidence.